Remarks/Arguments

Claims 1-31 are pending. Claims 1, 10, and 16 have been amended to more clearly and distinctly claim the subject matter that Applicants regard as their invention. Claims 29-31 are added to more fully claim the subject matter that applicants regard as their invention. Support for the amendments can be found, for example, in paragraphs [0019] -[0021] and Fig. 5. No new matter is believed to be added by the present amendment.

Claims 1-6, 10-13, 16-20, 23-27 are rejected under 35 U.S.C. § 103(a) as being unpatentable over US Patent 7,392,393 (hereinafter "Taki") and further in view of US Patent Application 20020131594 (hereinafter "Hori").

Claims 1-6, 10-13, 16-20, 23-27 are rejected under 35 U.S.C. § 103(a) as unpatentable over Taki in view of Hori. Applicants respectfully traverse this rejection for at least the following reasons.

Taki

The system of Taki pertains to a content distribution system where content is securely downloaded to a user device. Prior to the system downloading the content to the user device, the system verifies or authenticates that the user device is permitted to receive the downloaded content. This verification is done without directly communicating with the user device (see Abstract: *"thereby verifying the authenticity of the device serving as the download destination* ***without directly authenticating the device serving as the download destination"*** (emphasis added)).

Instead, the system of Taki uses a proxy method of authenticating the user device whereby the requesting device authenticates the user device through a series of exchanges between the requesting device and the content server (see col. 9, lines 1 – 7: *"[T]he user of the mobile information terminal 130 accesses the content distribution server 150 using the mobile information terminal 130, and* ***participates in a proxy authentication on behalf of the home PC 120*** *to prove that the home PC is a trusted user device and has legitimate right to access content"* (emphasis added)).

This is further evidenced in Figures 3, 7, 11, and 15 of Taki. In these figures, there is only one arrow pointing from the content distribution server to the Home PC (i.e., user device) and it is in one direction only – from the content distribution server to the Home PC -- to show the step of downloading the content to the HomePC . There is no other communication between the HomePC and the content distribution server.

Claimed Invention

By contrast, the claimed invention authenticates the destination device (i.e., remote site) through direct communications with the destination device. As shown in Fig. 2, there are several arrows going back and forth between the content customer (i.e., remote site) and the content server. This is because these exchanges include authenticating the content consumer (i.e., remote site) through direct communications with the content server. This is through the use of the access code. The access code or CAC (Content Access Credential) is provided to the content consumer by the content server. The content consumer (i.e., remote site) then transmits the access code back to the content server. Then the content server uses the access code to verify the content consumer (i.e., remote site) (see Fig. 5, step 550 performed first before steps 560 – 580).

The access code may also be used to indicate to the content server when to download the content (see paragraph [0019]: *"The CAC is used to access the requested content by the designated CC 150 at a later time"*; also see paragraph [0021]). When the content consumer wants to receive the content, it transmits the access code to the content server. The content server, in turn, downloads the content after verifying the access code or the content consumer (see Fig. 5, steps 540 – 550).

Amended claim 1 recites the following:

1. A device, located at a remote site in communication with a network having at least one server and a content requester, comprising:

a processor in communication with a memory, said processor operable to execute code for:

receiving a first information item comprising an access code and a content key scrambled using a key known by said device, said access code generated by said at least one server in response to a request for a second information item provided by the content requester;

descrambling said first information item using the key known by said device;

transmitting said access code to a server hosting said second information item; and

receiving said second information item scrambled using said content key after said server hosting the second information item verifies said access code.

Taki does not recite, teach, or suggest the access code.

The Examiner contends that the content-signing key of Taki corresponds to the claimed "access code." Applicants respectfully disagree. In Taki, the content-signing key is used to digitally sign the content and is used by the destination device to verify that the content was not tampered with (see Fig. 5, step S127 (the content is signed using the content signing key) and Fig. 6, step S134 (the content is verified using the content signing key)). Verification that the content has not been tampered and verification of a particular party are two entirely separate and distinct concepts in content security. By contrast, as noted above, the access code of the claimed invention is used to directly authenticate the remote site not the downloaded content.

With respect to the access code, amended claim 1 recites the following:

receiving a first information item comprising an access code and a content key scrambled using a key known by said remote site, ***said access code generated by said at least one server in response to a request for a second information item provided by the content requester;***

...

transmitting said access code to a server hosting said second information item; *and*

receiving said second information item scrambled using said content key ***after said server hosting the second information item verifies said access code.***

(Emphasis added).

As shown in amended claim 1 above (In bold italics), the remote device receives the access code that was generated by the server in response to a request for a second information item requested by the content requester (i.e., receiving first information step). The remote device then transmits the access code back to the server when the remote site is able to receive the second information item (i.e., transmitting step). The server verifies the access code, scrambles the second information item with the content key and transmits the scrambled second information item to the remote device (i.e., receiving said second information item step).

By contrast, the content signing key in Taki is used to descramble the content. Amended claim 1 recites that the remote site transmits the access code when the remote site wants to receive the content. The destination device in Taki does not directly communicate with the content server which means the destination device does not transmit an access code to the content server. Accordingly, for at least the above-mentioned reasons, the access code of amended claim 1 is not recited, taught, or suggested in Taki.

Hori does not recite, teach, or suggest the access code

Hori pertains to the playback of non-encrypted content not subject to a license (e.g., promotional audio to advertise the audio) when the content contains both encrypted content subject to a license and non-encrypted content not subject to a license. The problem of verifying, or authenticating, the device playing back the data is not the focus of Hori and as such, Hori does not recite, teach, or suggest the access code recited in the present claims.

No motivation to combine Taki and Hori

There is no motivation to combine Taki and Hori to come up with the claimed invention. This is because each solves a different problem and the combination would not produce the claimed invention. Hori is concerned with the playback of non-encrypted and encrypted data subject to different license restrictions and Taki is concerned with proxy authentication. In fact, Taki explicitly teaches away from the claimed invention. Taki explicitly recites that it uses "proxy authentication" of the destination device whereas the claimed invention uses direct communication

with the destination device to verify it. Accordingly, one skilled in the art would not look to these references since they address different problems, and thus, the features in the claimed invention are not recited, taught, or shown in these references.

Applicants submit that for at least the reasons discussed above, the suggested combination of Taki and Hori fail to disclose, teach, or suggest each and every feature recited in the independent claims and the claims that depend on them, are believed to be patentably distinguishable over any combination of Taki and Hori.

Claims 7-9, 14-15, 21, 28 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Taki in view of Hori and further in view of WO 02/32026A1, (hereinafter Henrick).

Claims 7-9, 14-15, 21, 28 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Taki in view of Hori and further in view of Henrick. Applicants respectfully traverse this rejection since Henrick is unable to remedy the deficiencies of Taki and Hori explained above in conjunction with amended claim 1. Accordingly, withdrawal of the rejection is respectfully requested.

Claim 22 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Taki in view of Hori and further in view of Kuriya et al (US 2001/0056404 A1, hereinafter Kuriya).

Claim 22 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Taki in view of Hori and further in view of Kuriya. Applicants respectfully traverse this rejection since Kuriya is unable to remedy the deficiencies of Taki and Hori explained above in conjunction with amended claim 1. Accordingly, withdrawal of the rejection is respectfully requested.

Conclusion

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited.

Customer No. 24498 Attorney Dor No.: PU030241
Final Office Action Date: October 14, 2009

It is believed that there are no additional fees due with regard to the filing of this response. However if there is an additional fee due, please charge the fee, or credit any overpayment, to Deposit Account No. 07-0832.

Respectfully submitted,
JUNBIAO ZHANG ET AL.

By: _____

Paul P. Kiel, Attorney
Reg. No. 40,677
Phone (609) 734-6815

Date: 1/12/10

Patent Operations
Thomson Licensing LLC
P.O. Box 5312
Princeton, New Jersey 08543-5312